

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-153870

(43) 公開日 平成9年(1997)6月10日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 H 1/02			H 0 4 H 1/02	E
H 0 4 L 9/32			H 0 4 L 9/00	6 7 3 B
H 0 4 N 7/167			H 0 4 N 7/167	Z

審査請求 有 請求項の数12 O L (全 11 頁)

(21) 出願番号 特願平8-210371

(22) 出願日 平成8年(1996)8月9日

(31) 優先権主張番号 1 0 0 0 9 6 4

(32) 優先日 1995年8月10日

(33) 優先権主張国 オランダ (N L)

(71) 出願人 591104918

コニンクリジケ ビーティーティー ネー  
ダーランドエヌ ビーKONINKI JKE PTT NEDE  
RLAND NEAMLOZE VENN  
OOTSHAPオランダ国 9726 エイシー グローニゲ  
ン ステーションズウエー 10

(72) 発明者 ヨハン パン ティルバルジ

オランダ国 2719 ケイケイ ソエターメ  
ール プラタッホウト 64

(74) 代理人 弁理士 斉藤 武彦

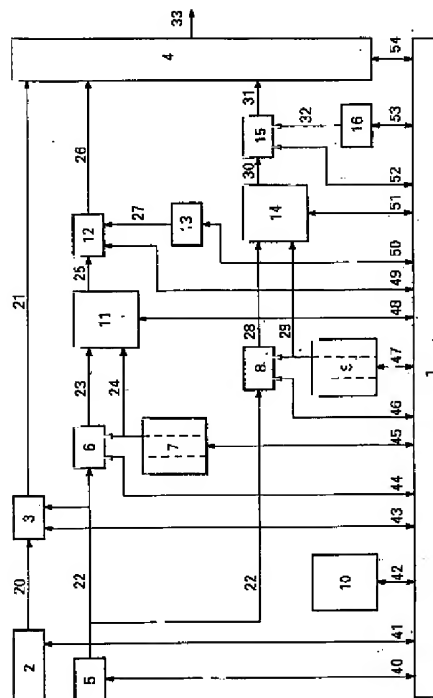
最終頁に続く

(54) 【発明の名称】 受信装置のほか送信装置ならびに、暗号化／翻訳メッセージにより、情報へのアクセスを得る方法

(57) 【要約】

【課題】 情報へのアクセスが、より能率的な方法で行われる方法を提供する。

【解決手段】 公認使用者ごとに、暗号化／翻訳メッセージにより、情報へのアクセスを得る周知の方法は、公認使用者のみが翻訳方法を行うので、使用者のみにより翻訳される暗号化メッセージを送信する。同じメッセージをすべての使用者に送信し、このメッセージは、使用者が公認されていないければ使用者に関連する暗号化方法により使用者ごとに暗号化され、使用者が公認されている暗号化されず、使用者は使用者に関連する翻訳方法を行わず他の使用者に関連する翻訳方法を行い、すべての使用者はこの同じメッセージを受信するが、公認使用者のみが暗号化メッセージを翻訳し、この翻訳されたメッセージにより情報へのアクセスを得ることができ、非公認使用者はそれらのためなお暗号化されたメッセージにより情報へのアクセスを得ることができず、この方法は能率的である。



**【特許請求の範囲】**

【請求項1】 暗号化／翻訳メッセージにより、公認使用者には情報へのアクセスを与え、非公認使用者には情報へのアクセスを与えない方法において、非公認使用者ごとに、前記非公認使用者に関連する暗号化方法によりメッセージ非公認使用者ごとに、前記非公認使用者に関連する暗号化方法によりメッセージを暗号化する工程、公認使用者ごとに、前記公認使用者に関連する暗号化方法によりメッセージを暗号化しない工程、使用者にメッセージを送信する工程、

各使用者が該使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため当該使用者に関連する翻訳方法を行わず、一方他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行う様に、使用者によりメッセージを受信する工程、

少なくとも一人の非公認使用者の場合には、公認使用者ごとに、前記非公認使用者に関連する暗号化方法により暗号化されたメッセージを翻訳し、前記公認使用者により、翻訳メッセージによる情報へのアクセスを得る工程、

非公認使用者でない場合には、公認使用者ごとに、前記公認使用者により、非暗号化メッセージによる情報へのアクセスを得る工程、および非公認使用者により、暗号化メッセージによる情報へのアクセスを得ない工程を備えることを特徴とする方法。

【請求項2】 情報は非暗号化メッセージにより暗号化され、非暗号化または翻訳メッセージによってのみ翻訳されることを特徴とする請求項1の方法。

【請求項3】 メッセージは、もう1つの暗号化方法により送信前に暗号化され、受信後の暗号化メッセージは、もう1つの翻訳方法により翻訳されることを特徴とする請求項1または2の方法。

【請求項4】 全数の使用者は多数の使用者群にわたり分配され、メッセージは使用者群ごとに送信されることを特徴とする請求項1、2または3の方法。

【請求項5】 公認使用者には情報へのアクセスを与え、非公認使用者には情報へのアクセスを与えないためデータメッセージを使用者に送信する送信装置において、この送信装置は、

使用者ごとに、前記使用者に関連する暗号化方法によりデータメッセージを暗号化可能とする暗号化装置、およびデータメッセージに使用者確認信号を加算する加算装置を備え、送信装置は、

使用者ごとに、非公認使用者の場合には第1値を有し公認使用者の場合には第2値を有する固有識別信号を発生する発生装置を備え、暗号化装置は、第1値を有する固有識別信号にตอบสนองして、前記非公認使用者に関連する暗号化方法によるデータメッセージを暗号化し、第2値を

有する固有識別信号にตอบสนองして、前記公認使用者に関連する暗号化方法によるデータメッセージを暗号化しない、固有識別信号を使用者ごとに受信する制御入力を用意することを特徴とする送信装置。

【請求項6】 送信装置は、データメッセージにより、使用者に送信される情報を暗号化する暗号化手段を備えることを特徴とする請求項5の送信装置。

【請求項7】 送信装置は、もう1つの暗号化方法によりメッセージを暗号化する暗号化装置に結合されるもう1つの暗号化装置を備えることを特徴とする請求項5または6の送信装置。

【請求項8】 全数の使用者は多数の使用者群にわたり分配され、送信装置は使用者群ごとにデータメッセージを送信することを特徴とする請求項5、6または7の送信装置。

【請求項9】 公認使用者には情報へのアクセスを与え、非公認使用者には情報へのアクセスを与えないデータメッセージを受信する受信装置において、受信装置は、データメッセージの加えられる使用者確認信号を検出する検出装置を備え、受信装置は、

使用者確認信号から、非公認他の使用者の場合には第1値を有し公認他の使用者の場合には第2値を有する他の使用者に関連する少なくとも1つの固有識別信号を検出する検出装置に結合されるもう1つの検出装置、および第1値を有する他の使用者に関連する少なくとも1つの固有識別信号にตอบสนองして、前記非公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳して、第2値を有する他の使用者に関連する少なくとも1つの固有識別信号にตอบสนองして、前記公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳しない、もう1つの検出装置に結合される翻訳装置を備えることを特徴とする受信装置。

【請求項10】 受信装置は、翻訳または非暗号化データメッセージにより、受信情報を翻訳する翻訳手段を備えることを特徴とする請求項9の受信装置。

【請求項11】 受信装置は、もう1つの翻訳方法によりメッセージを翻訳する翻訳装置に結合されるもう1つの翻訳装置を備えることを特徴とする請求項9または10の受信装置。

【請求項12】 全数の使用者は多数の使用者群にわたり分配され、受信装置は、ある使用者群に関連するデータメッセージを検出する検出手段を備えることを特徴とする請求項9、10または11の受信装置。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】 本発明は、暗号化／翻訳メッセージにより、公認使用者には情報へのアクセスを与え、非公認使用者には情報へのアクセスを与えない方法

に関する。

【0002】

【従来の技術】このような方法は一般的な知識であり、つぎのように実行する。もし使用者が公認されていれば、使用者は暗号化メッセージを翻訳する翻訳方法を行うが、もし使用者が公認されていなければ、使用者は翻訳方法を行わない。その結果、公認使用者はメッセージを翻訳し、この翻訳メッセージにより使用者にある情報へのアクセスを与えるが、非公認使用者はメッセージを翻訳できず、その結果、使用者は情報へのアクセスを得られない。前記情報は、たとえば、メッセージに記録され、または、たとえば、使用者が翻訳メッセージを返した後のみに使用者に送信され、または、たとえば、暗号化状態で使用者に送信され、前記使用者は翻訳メッセージにもとずいてのみ暗号化情報を翻訳できる。

【0003】このような方法は、とりわけ、公認使用者ごとに、メッセージが送信されねばならず、数ノードに接続される多くの使用者の場合には、多くのメッセージが順次送信されることになり、周知の方法は非能率的になり、各使用者は通過するすべての（暗号化）メッセージを付加的に見るといふ、欠点を有する。

【0004】文献：

EP 0 641 103

1994年8月21-25日、米国カルフォルニア州サンタバーバラ、第14年度国際暗号会議、暗号の進歩、クリプト'94、ベニイ コール、アモス フィアットおよびモニ ナオルによる”トレーシングトレーター”  
1993年8月23-25日、米国カルフォルニア州サンタバーバラ、第13年度国際暗号会議、暗号の進歩、クリプト'93、アモス フィアットおよびモニ ナオルによる”放送暗号”

1992年、IEEEプレス、グスタブスJ. シモンズ編集、情報保科学、”現代の暗号”

1982年、ジョン ウイリー・アンド・サン、ウィリー・インターサイエンス刊行物、カールH. メイヤーおよびステフェンM. メチアスによる、安全システムの設計および実施のガイド、”暗号術：コンピューターデータ安全の新次元”すべて文献はこの特許出願に組み込まれる。

【0005】

【発明が解決しようとする課題】本発明の目的は、とりわけ、情報へのアクセスが、より能率的な方法で行われる、頭書に記載した種類の方法を提供することにある。

【0006】

【課題を解決するための手段】この目的のため、本発明による方法は、非公認使用者ごとに、前記非公認使用者に関連する暗号化方法によりメッセージを暗号化する工程、公認使用者ごとに、前記公認使用者に関連する暗号化方法によりメッセージを暗号化しない工程、使用者にメッセージを送信する工程、各使用者が前記使用者に關

連する暗号化方法により暗号化されたメッセージを翻訳するため前記使用者に関連する翻訳方法を行わず、一方他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行い、使用者によりメッセージを受信する工程、少なくとも一人の非公認使用者の場合には、公認使用者が前記非公認使用者に関連する暗号化方法により暗号化されたメッセージを翻訳し、前記公認使用者により、翻訳メッセージによる情報へのアクセスを得る工程、非公認使用者でない場合には、公認使用者ごとが、前記公認使用者により、非暗号化メッセージによる情報へのアクセスを得る工程、および非公認使用者により、暗号化メッセージによる情報へのアクセスを得ない工程を備えることを特徴とする。

【0007】同じメッセージを当該使用者に送信することによって、このメッセージは、前記使用者が公認されてなければ前記使用者に関連する暗号化方法により使用者ごとに暗号化され、前記使用者が公認されていれば前記使用者に関連する暗号化方法により暗号化されないものであり、当使用者はこの同じメッセージを受信するが、各使用者は前記使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記使用者に関連する翻訳方法を行わず、他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行い、公認使用者のみが暗号化メッセージを翻訳できその翻訳されたメッセージにより情報へのアクセスを得ることができ、非公認使用者は、なお暗号化されたメッセージにより情報へのアクセスを得ることができず、非公認使用者でない場合には、もちろん、すべての公認使用者は非暗号化メッセージによる情報へのアクセスを得ることができある。その結果、同一のメッセージのみが当使用者に送信されねばならず、本発明による方法はきわめて能率的である。

【0008】本発明は、とりわけ、つぎの暗号化メッセージを送信するつぎの使用者ごとよりもすべての使用者（公認使用者のみが、翻訳メッセージにより、情報へのアクセスを得ることができる）に同一の暗号化メッセージをかなり能率よく送信するという識見にもとずいている。

【0009】周知の方法が非能率的であるという問題は同じメッセージを当使用者に送信することにより解決され、このメッセージは、使用者が公認されていなければ前記使用者に関連する暗号化方法により使用者ごとに暗号化され、前記使用者が公認されていれば暗号化されないものであり、この場合、各使用者は前記使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記使用者に関連する翻訳方法を行わされず、他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行わなければならない。

【0010】本発明による第1実施例は、情報は非暗号化メッセージにより暗号化され、非暗号化または翻訳メッセージによってのみ翻訳されることを特徴とする。

【0011】非暗号化メッセージにより情報を暗号化することにより、このようにして暗号化された情報のみが、非暗号化または翻訳メッセージにより翻訳されることができ、公認使用者のみが前記情報へのアクセスを得る。

【0012】本発明による第2実施例は、メッセージは、もう1つの暗号化方法により送信前に暗号化され、受信後の暗号化メッセージは、もう1つの翻訳方法により翻訳されることを特徴とする。

【0013】もう1つの暗号化方法により送信前に暗号化することによって、もう1つの翻訳方法によりその翻訳を受信後、メッセージは、すべての当使用者が公認されていても、暗号化状態で常に送信されるので、安全性が得られる。

【0014】本発明による第3実施例は、全数の使用者は多数の使用者群にわたり分配され、メッセージは使用者群ごとに送信されることを特徴とする。

【0015】多数の使用者群にわたり全数の使用者を分配することにより、1つのメッセージは使用者群ごとに送信され、各使用者は明らかに、丁度使用者群と同じ多くの通過するメッセージを見るが、前記使用者はその使用者に関連するメッセージを翻訳するだけよく、また前記使用者は同じ使用者群に属するすべての他の使用者に関連する数の翻訳方法を行うだけでよい。

【0016】本発明はさらに、公認使用者には情報へのアクセスを与え非公認使用者には情報へのアクセスを与えないためデータメッセージを使用者に送信する送信装置において、この送信装置は、使用者ごとに、前記使用者に関連する暗号化方法によりデータメッセージを暗号化可能とする暗号化装置、およびデータメッセージに使用者確認信号を加算する加算装置を備える、送信装置に関する。

【0017】このような送信装置は一般的知識のものでつぎのように作動する。使用者ごと暗号化装置により、データメッセージは前記使用者に関連する暗号化方法により暗号化され、使用者確認信号は加算装置によりデータメッセージに加算され、暗号化データメッセージは前記使用者に送信される。使用者が公認されていれば、暗号化データメッセージを翻訳するため翻訳方法を実行するが、前記使用者が公認されていなければ、翻訳方法を実行しない。その結果、公認使用者はデータメッセージを翻訳し、翻訳データメッセージにより使用者にある情報へのアクセスをさせるが、非公認使用者はデータメッセージを翻訳できず、その結果情報へのアクセスを得られない。

【0018】このような送信装置は、とりわけ、公認使用者ごとに1つのデータメッセージが送信されねばなら

ず、数ノードに接続される多くの使用者の場合には、多くのデータメッセージが順次送信されることになり、装置全体が非能率的になり、さらに各使用者は、通過するすべての(暗号化)メッセージを見ると言う欠点がある。

【0019】本発明の目的は、とりわけ、情報へのアクセスがより能率的に進められる、上記種類の送信装置を提供することにある。

【0020】この目的のため、本発明による送信装置は、使用者ごとに、非公認使用者の場合には第1値を有し公認使用者の場合には第2値を有する固有識別信号を発生する発生装置を備えると共に、暗号化装置を備え、該暗号化装置は、第1値を有する固有識別信号に応答して、前記非公認使用者に関連する暗号化方法によるデータメッセージを暗号化し、第2値を有する固有識別信号に応答して、前記公認使用者に関連する暗号化方法によるデータメッセージを暗号化しない、固有識別信号を使用者ごとに受信する制御入力を備えることを特徴とする。

【0021】発生装置により、非公認使用者の場合には第1値を有し、公認使用者の場合には第2値を有する使用者ごとの固有識別信号を発生することにより、暗号化装置は、第1値を有する固有識別信号に応答して、前記非公認使用者に関連する暗号化方法によるデータメッセージを暗号化し、第2値を有する固有識別信号に応答して、前記公認使用者に関連する暗号化方法によるデータメッセージを暗号化しない、固有識別信号を使用者ごとに受信する制御入力を備え、それで、同じデータメッセージは当使用者に送信され、このデータメッセージは、使用者が公認されていなければ使用者に関連する暗号化方法により使用者ごとに暗号化され、使用者が公認されていれば暗号化されず、当使用者はこの同じデータメッセージを受信する。各使用者が、使用者の暗号化方法により暗号化されたデータメッセージを翻訳するために使用者に関連する翻訳方法を行わず、他の使用者に関連する暗号化方法により暗号化されたデータメッセージを翻訳するために他の使用者に関連する翻訳方法を行えば、公認使用者のみが暗号化データを翻訳し、翻訳されたデータメッセージにより情報へのアクセスを得、非公認使用者はなお暗号化されたデータメッセージによる情報へのアクセスは得られず、非公認使用者でない場合には、もちろん、すべての公認使用者は非暗号化データメッセージにより情報へのアクセスを得ることができる。その結果、同一データメッセージのみが当使用者に送信されればよく、本発明による全体はきわめて能率がよい。

【0022】本発明による送信装置の第1実施例は、送信装置がデータメッセージにより、使用者に送信される情報を暗号化する暗号化手段を備えることを特徴とする。

【0023】暗号化手段により情報を暗号化することに

より、暗号化された情報は非暗号化または翻訳データメッセージによってのみ翻訳され、公認使用者のみが情報へのアクセスを得る。

【0024】本発明による送信装置の第2実施例は、送信装置が、もう1つの暗号化方法によりメッセージを暗号化する暗号化装置に結合されるもう1つの暗号化装置を備えることを特徴とする。

【0025】もう1つの暗号化装置により送信前にデータメッセージを暗号化することにより、受信後、もう1つの翻訳方法により翻訳されねばならず、データメッセージは、すべての当使用者が公認されていても暗号化状態で常に送信され、安全である。

【0026】本発明による送信装置の第3実施例は、全数の使用者が多数の使用者群にわたり分配され、送信装置は使用者群ごとにデータメッセージを送信することを特徴とする。

【0027】多数の使用者群にわたり全数の使用者を分配することにより、送信装置は使用者群ごとに1つのデータメッセージを送信し、各使用者は明らかに、使用者群と度度同じ多くの通過するデータメッセージを見るが、前記使用者のみがその使用者群に関連するデータメッセージを翻訳すればよく、前記使用者のみが同じ使用者群に属するすべての他の使用者に関連する数の翻訳方法を行えばよい。

【0028】本発明はさらに、公認使用者には情報へのアクセスを与え非公認使用者には情報へのアクセスを与えないデータメッセージを受信する受信装置において、受信装置は、データメッセージの加えられる使用者確認信号を検出する検出装置を備える、受信装置に関する。

【0029】このような受信装置は一般的知識のもので、つぎのように作動する。使用者ごと、送信装置により、データメッセージは前記使用者に関連する翻訳方法により翻訳され、使用者確認信号は送信装置によりデータメッセージに加算され、暗号化し修正したデータメッセージは前記使用者に送信される。検出装置により、データメッセージに加えられる使用者確認信号が検出され、それににもとずいて、前記データメッセージが前記受信装置にたいするものかどうかを設定される。使用者が公認されていれば、受信装置は暗号化データメッセージを翻訳するために翻訳方法を行うが、使用者が公認されていなければ、受信装置は翻訳方法を行わない。その結果、公認使用者はデータメッセージを翻訳し、この翻訳データメッセージにより使用者にある情報へのアクセスをさせるが、非公認使用者はデータメッセージを翻訳できず、その結果使用者は情報へのアクセスはできない。

【0030】このような受信装置は、とりわけ、公認使用者ごとに1つのデータメッセージが送信されねばならず、数ノードに接続される多くの使用者の場合には、多くのデータメッセージが順次送信されることになり、既

知全体が非能率的になり、さらに各使用者は、通過するすべての（暗号化）メッセージを見ると言う欠点がある。

【0031】本発明の他の目的は、とりわけ、情報へのアクセスがより能率的に進められる、上記種類の受信装置を提供することにある。

【0032】この目的のため、本発明による受信装置は、使用者確認信号から、非公認他の使用者の場合には第1値を有し公認他の使用者の場合には第2値を有する他の使用者に関連する少なくとも1つの固有識別信号を検出する検出装置に結合されるもう1つの検出装置、および第1値を有する他の使用者に関連する少なくとも1つの固有識別信号に応答して、前記非公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳して、第2値を有する他の使用者に関連する少なくとも1つの固有識別信号に応答して、前記公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳しない、もう1つの検出装置に結合される翻訳装置を備えることを特徴とする。

【0033】使用者確認信号からもう1つの検出装置により、非公認他の使用者の場合には第1値を有し公認他の使用者の場合には第2値を有する他の使用者に関連する少なくとも1つの固有識別信号を検出し、および第1値を有する他の使用者に関連する少なくとも1つの固有識別信号に応答する翻訳装置により、前記非公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳して、第2値を有する他の使用者に関連する少なくとも1つの固有識別信号に応答して、前記公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳しないことにより、同じデータメッセージは当使用者に送信され、このデータメッセージは使用者が公認されていなければ、使用者に関連する暗号化方法により使用者ごとに暗号化され、使用者が公認されていれば、暗号化されず、当使用者はこの同じデータメッセージを受信する。公認使用者のみが暗号化データメッセージを翻訳し、翻訳されたデータメッセージにより情報へのアクセスを得るが、非公認使用者でない場合には、もちろん、すべての公認使用者は非暗号化データメッセージにより情報へのアクセスを得る。その結果、同一のデータメッセージのみを当使用者に送信すればよく、本発明による全体はきわめて能率的である。

【0034】本発明による受信装置の第1実施例は、翻訳または非暗号化データメッセージにより、受信情報を翻訳する翻訳手段を備えることを特徴とする。

【0035】送信装置により情報を暗号化することにより、このように暗号化された情報のみが翻訳手段により翻訳され、公認使用者のみが情報へのアクセスを得る。

【0036】本発明による受信装置の第2実施例は、もう1つの翻訳方法によりメッセージを翻訳する翻訳装置に結合される、もう1つの翻訳装置を備えることを特徴

とする。

【0037】データメッセージが送信装置により送信前に暗号化されれば、受信後、もう1つの翻訳装置により翻訳されねばならず、データメッセージは、すべての当使用者が公認されていても暗号化状態で常に送信され、安全である。

【0038】本発明による受信装置の第3実施例は、全数の使用者は多数の使用者群にわたり分配され、受信装置は、ある使用者群に関連するデータメッセージを検出する検出手段を備えることを特徴とする。

【0039】全数の使用者を多数の使用者群にわたり分配することにより、送信装置は使用者群ごとに1つのデータメッセージを送信し、各使用者は明らかに使用者群と丁度同じ多くの通過するデータメッセージを見るが、前記使用者は、検出手段により、検出し、使用者群に関連するデータメッセージのみを翻訳せねばならず、使用者は、同じ使用者群に属するすべての他の使用者に関連する数の翻訳方法のみを行わねばならない。

【0040】EP-0641103は選択送信システムにおけるキーを分配する方法および装置を開示する。この場合、各受信者はそれ自身のキーでなくすべての他の受信者のキーを扱う。組み合わせキーによる送信者は暗号化情報を送信し、この組み合わせキーはすべての非公認受信者に属するキーのモジュロ2付加により得られる。非公認受信者はそれら自身のキーを扱わないので、どの受信者が非公認であるかを知って、組み合わせキーを模倣できないが、公認受信者は、どの受信者が非公認であるかを知って、組み合わせキーを模倣し、その結果、暗号化情報は、組み合わせキーにより、公認受信者のみにより翻訳できる。その欠点は、とりわけ、授権の付加/除去により、情報が暗号化される変型組み合わせキーとなり、その結果、前記授権の付加/除去は発生する大きな技術的問題なしに極めて限られた数のモーメントでのみ行うか、または任意のモーメントで生ずるかであり、大きな技術的問題を含む。この特許には本発明による方法も本発明による装置のいずれも開示されていない。

【0041】

【実施例】以下、本発明を、図に示す典型実施例を参照して詳細に説明する。ここで、図1は本発明による方法に適用する本発明による送信装置を示し、図2は本発明の方法に適用する本発明による受信装置を示す。

【0042】図1に示す本発明による送信装置は、制御接続部41により、プロセッサ1に結合され、その出力が、接続部20により、暗号化手段3の第1入力に結合される情報源2を備える。さらにまた図1に示す本発明による送信装置は、制御接続部4により、プロセッサ1に結合され、その出力が、接続部22により、暗号化手段3の第2入力と、第1暗号化装置6の第1入力と、第2暗号化装置6の第1入力とに結合されるメッセ

ージメモリ5を備える。プロセッサメモリ10は、制御接続部42により、プロセッサ1に結合され；暗号化手段3は、制御接続部43により、プロセッサ1に結合され；第1暗号化装置6は、制御接続部44により、プロセッサ1に結合され；第2暗号化装置8は、制御接続部46により、プロセッサ1に結合される。暗号化手段3の出力は、接続部21により、マルチプレクサー4の第1入力に結合される。第1暗号化装置6の第1入力は、接続部24を介して、制御接続部45によりプロセッサ1に結合される第1テーブルメモリ7の出力に接続される。第2暗号化装置8の第2入力は、接続部29により、制御接続部47によりプロセッサ1に結合される第2テーブルメモリ9の接続される。第1暗号化装置6の出力は、接続部23により、制御接続部48によりプロセッサ1に結合され、その第2入力が接続部24により第1テーブルメモリ7の出力に接続される第1加算装置11の第1入力に結合される。第2暗号化装置8の出力は、接続部28により、制御接続部51によりプロセッサ1に結合され、その第2入力が接続部29により第2テーブルメモリ9の出力に接続される第2加算装置14の第1入力に結合される。第1加算装置11の出力は、接続部25により、制御接続部49によりプロセッサ1に結合され、その第2入力が接続部27により、制御接続部50によりプロセッサ1に結合される第1コードメモリ13の出力に接続される第3暗号化装置12の第1入力に結合される。第2加算装置14の出力は、接続部30により、制御接続部52によりプロセッサ1に結合され、その第2入力が接続部32により、制御接続部53によりプロセッサ1に結合される第2コードメモリ16の出力に接続される第4暗号化装置15の第1入力に結合される。第3暗号化装置12の出力は、接続部26によりマルチプレクサー4の第2入力に結合され、第4暗号化装置15の出力は、接続部31により、その出力が接続部33に接続され、制御接続部54によりプロセッサ1に結合されるマルチプレクサー4の第3入力に結合される。

【0043】図1に示す送信装置の作動は次の通りである。送信されるペーパTVビデオ信号は情報源2に格納される。その送信前に、公認の人または第1使用者群に属する使用者でない人は第1テーブルメモリ7に記録され、公認の人または第2使用者群に属する使用者でない人は第2テーブルメモリ9に記録される。この目的のため、両テーブルメモリ7と9各々は3つのコラム、すなわち、使用者識別を格納する行ごとの第1コラム、公認の人または関連使用者でない人を格納する行ごとの第2コラム、および関連使用者に結合される暗号化方法を格納する行ごとの第3コラムを有する。一般に、第1および第3コラムに格納されるデータは既に存在するかまたは長期間格納されるが、第2コラムに必要なデータは送信されるペーパTVビデオ信号ごとに設定され両テーブ



ルメモリ7と9にロードされねばならない。これは制御接続部45、47およびプロセッサ1により行われる。送信されるペーTVビデオ信号ごとに、制御接続部40およびプロセッサ1により、メッセージメモリ5にロードされるメッセージがさらに設定される。

【0044】メッセージメモリ5は、制御接続部40により、プロセッサ1から生ずる指令信号を受信して、それに応答して、接続部22により暗号化手段3、第1暗号化装置6および第1暗号化装置8に送られる格納メッセージを発生する。暗号化手段3はさらに、接続部20により、制御接続部41により受信される指令信号に応答して情報源2により送信される情報源2から生じかつプロセッサ1から生ずるペーTVビデオ信号を受信し、制御接続部43により受信される制御信号の制御の下にメッセージにもとずきかつプロセッサ1から生ずる前記ペーTVビデオ信号を暗号化して、その後暗号化ビデオ信号は接続部21によりマルチプレクサー4に送られる。

【0045】第1テーブルメモリ7は、制御接続部45により、プロセッサ1から生ずる指令信号を受信し、引き続き、それに応答して、第1群識別および行ごと（または使用者識別ごと）に格納されているデータ（の一部）を発生し、第1群識別、すべての使用者識別および行ごと（または使用者識別ごと）第1と第2コラムに格納される使用者公認が、接続部24により、第1加算装置11に送られる一方、第3コラムに格納される暗号化方法のうち、非公認使用者に関連する暗号化方法のみが接続部24により第1暗号化装置6に送られる。制御接続部44により受信され、プロセッサ1から発する制御信号の制御の下、第1暗号化装置6は、非公認使用者に関連する暗号化方法により、たとえば、前記暗号化方法のある順序でメッセージに引き続き与えることにより受信メッセージを暗号化する。その後、第1暗号化装置6は、プロセッサ1の制御の下、暗号化されたメッセージを第1の仕方で接続部23により第1加算装置11に送る。第1加算装置11は、プロセッサ1から生じ制御接続部48により受信される制御信号に応答して、第1の仕方で暗号化されたメッセージを、第1テーブルメモリ7に格納される第1群識別、すべての使用者識別および使用者公認と組み合わせ、プロセッサ1の制御の下、組み合わせ全体を接続部25により第3暗号化装置12に送る。第1コードメモリ13は、制御接続部50により、プロセッサ1から発する指令信号を受信して、それに応答して、接続部27により第3暗号化装置12に送られる第1コードを発生する。制御接続部49により受信されプロセッサ1から生ずる制御信号の制御の下、第3暗号化装置12は第1コードにもとずいて到来組み合わせ全体を暗号化する。その後、第3暗号化装置12はプロセッサ1の制御の下、第1コードにより暗号化された全体を接続部26によりマルチプレ

クサー4に送る。

【0046】第2テーブルメモリ9は、制御接続部47により、プロセッサ1から生ずる指令信号を受信し、引き続き、それに応答して、第2群識別および行ごと（または使用者識別ごと）に格納されるデータ（の一部）を発生し、第2群識別、すべての使用者識別および行ごと（または使用者識別ごと）に第1と第2コラムに格納される使用者公認が、接続部29により、第2加算装置14に送られる一方、第3コラムに格納される暗号化方法のうち、非公認使用者に関連する暗号化方法のみが接続部29により第2暗号化装置8に送られる。制御接続部46により受信され、プロセッサ1から発する制御信号の制御の下、第2暗号化装置8は、非公認使用者に関連する暗号化方法により、たとえば、前記暗号化方法のある順序でメッセージに引き続き与えることにより受信メッセージを暗号化する。その後、第2暗号化装置8は、プロセッサ1の制御の下、暗号化されたメッセージを第2の仕方で接続部28により第2加算装置14に送る。第2加算装置14は、プロセッサ1から生じ制御接続部51により受信される制御信号に応答して、第2の仕方で暗号化されたメッセージを、第2テーブルメモリ9に格納される第2群識別、すべての使用者識別および使用者公認と組み合わせ、プロセッサ1の制御の下、組み合わせ全体を接続部30により第4暗号化装置15に送る。第2コードメモリ16は、制御接続部53により、プロセッサ1から発する指令信号を受信して、それに応答して、接続部27により第4暗号化装置12に送られる第2コードを発生する。制御接続部52により受信されプロセッサ1から生ずる制御信号の制御の下、第4暗号化装置15は第2コードにもとずいて到来した組み合わせ全体を暗号化する。その後、第4暗号化装置15はプロセッサ1の制御の下、第2コードにより暗号化された全体を接続部31によりマルチプレクサー4に送る。

【0047】制御接続部54により受信され、プロセッサ1から生ずる制御信号の制御の下、マルチプレクサー4は暗号化ビデオ信号を、第1コードにより暗号化された全体および第2コードにより暗号化された全体と組み合わせた後、その結果を、接続部33により、少なくとも第1および第2使用者群に属する使用者に送信される。

【0048】本発明による図2に示す受信装置は、その入力が接続部33に接続され、制御接続部140によりプロセッサ100に結合されるデマルチプレクサー101を備える。デマルチプレクサー101の第1出力は、接続部120により、制御接続部147によりプロセッサ100に結合される翻訳手段102の第1入力に結合される。翻訳手段102の出力はたとえばテレビジョンセット等情報プロセッサに結合するため接続部121に接続され、翻訳手段102の第2入力は接続部

127により第1翻訳装置107の出力に接続される。第1翻訳装置107の第1入力は接続部125により分割装置105の第1出力に結合され、第1翻訳装置107の第2の入力は接続部128により、制御接続部146によりプロセッサ100に結合される第3テーブルメモリ108の出力に接続される。制御接続部145により第1翻訳装置107はプロセッサ100に結合される。分割装置105の第2出力は、接続部126により、制御接続部144によりプロセッサ100に結合されるデータメモリ106の入力に結合される。分割装置105の入力は、接続部124により、第2翻訳装置103の出力に接続され、一方分割装置105は制御接続部143により、プロセッサ100に結合される。第2翻訳装置103の第1入力は接続部122によりデマルチプレクサ101の第2出力に結合され、第2入力は接続部123により、制御接続部142によりプロセッサ100に結合される第3コードメモリ104の出力に接続される。制御接続部141により、第2暗号化装置103はプロセッサ100に結合される。

【0049】図2に示す受信装置の作動は次の通りである。ここで、この受信装置は第1使用者群に属する公認使用者に関連するものと想定する(送信装置では、メッセージは前記公認使用者に関連する暗号化方法により暗号化されないで、他の非公認使用者に関連する暗号化方法により多分暗号化される)。制御接続部140により受信されプロセッサ100から生ずる制御信号の制御の下、デマルチプレクサ101は暗号化ビデオ信号を、第1コードにより暗号化された全体および第2コードにより暗号化された全体から分離した後、暗号化ビデオ信号は、接続部120により翻訳手段102に送られ、第1コードにより暗号化された全体は接続部122により第2翻訳装置103に送られる。第3コードメモリ104は制御接続142により、プロセッサ100から生ずる指令信号を受信し、それに応答して、接続部123により第2翻訳装置103に送られる第3コードを発生する。制御接続部141により受信されプロセッサ100から生ずる制御信号の制御の下、第2翻訳装置103は第3コードにもとずいて第1コードにより翻訳された全体を翻訳する。一般に、この場合、第1コードと第3コードとは等しい。つぎに、第2翻訳装置103は、プロセッサ100の制御の下、第3コードにより翻訳された全体を、接続部124により分割装置105に送る。

【0050】分割装置105は、プロセッサ100から生じ制御接続部143により受信される制御信号に応答して、第3コードにより翻訳された全体を、一方で、第1の仕方で暗号化されたメッセージに、他方で第1群識別、すべての使用者識別および使用者公認に分割し、プロセッサ100の制御の下、第1の仕方で暗号化されたメッセージを第1翻訳装置107に送り、プロセッ

サ100の制御の下第1群識別、すべての使用者識別および使用者公認を接続部126によりデータメモリ106に送る。プロセッサ100は、制御接続部144により、第1群識別が(たとえば、テーブルメモリ108に格納され、制御接続部146によりプロセッサ100に送られる(第1群識別を一致せねばならない)第3群識別と比較することによって)データメモリ106に格納されていることを検出し、その結果、前記データが全く前記受信装置に意図されていることが設定される。

【0051】第3テーブルメモリ108は3つのコラム、すなわち、使用者識別を格納する行ごとの第1コラム、公認の人または関連使用者でない人を格納する行ごとの第2コラム、および関連使用者に結合される暗号化方法を格納する行ごとの第3コラムを有する。一般に、第1および第3コラムに格納されるデータは既に存在するかまたは長期間格納されるが、第2コラムに必要なデータは送信されるペーTVビデオ信号ごとに設定され、テーブルメモリ108にロードされねばならない。これは、プロセッサ100の制御の下、データメモリ106に格納される使用者識別および使用者公認を制御接続144により、プロセッサ100により、および制御接続146により第3テーブルメモリ108に送ることにより行われる。

【0052】第3テーブルメモリ108は、制御接続部146により、プロセッサ100から生ずる指令信号を受信して、それに応答して第3コラムに格納される行ごと(または使用者識別ごと)にデータ(の一部)を受信する一方、第3コラムに格納される翻訳方法のうち、非公認使用者に関連する翻訳公報のみが、接続部128により、第1翻訳装置107に送られる。制御接続部145により受信されプロセッサ100から生ずる制御信号の制御の下、第1翻訳装置107は、非公認使用者に関連する翻訳方法による暗号化メッセージを、たとえば、(送信装置とは逆の)ある順序で前記翻訳方法にメッセージを引き続き与えることによって、翻訳する。つぎに、第1翻訳装置107は、プロセッサ100の制御の下、翻訳メッセージを、接続部127により翻訳手段102に送る。

【0053】翻訳手段102は、制御接続部147により、プロセッサ100から生ずる制御信号を受信し、それに応答して、接続部127により受信される翻訳メッセージにもとずいて暗号化ビデオ信号を翻訳した後、元のペーTVビデオ信号は接続部によりまた、たとえば、テレビジョンセットにより観察される。

【0054】他の(第2の)使用者群に意図される、第2コードにより送信装置で暗号化される全体に関する限り、図2に示す受信装置の作動には、少なくとも3つの作動がある。第1に、デマルチプレクサ101は、たとえば、ある時間間隔を無視することにより既に選択



し、それで第2コードにより暗号化される全体はデマルチプレクサー101を通らない。第2に、第2コードにより送信装置で暗号化される全体は、たとえば、やがて、第1コードにより暗号化される全体から分離されるので、デマルチプレクサー101を通り、さらに、第1コードにより暗号化される全体が提供された後いつか、第2翻訳装置103に提供される一方、第2コードは第3コードメモリに格納される第3コードとは異なるので、この時、ここでは正しい翻訳が行われず、その結果分割装置105および（または）データメモリ106は意味のないことに対処しなければならない。

【0055】第3に、第1コードにより暗号化される全体は、たとえば、やがて、第1コードにより暗号化される全体から分離されるので、デマルチプレクサー101を通り、さらに、第1コードにより暗号化される全体が提供された後いつか、第2翻訳装置103に提供される一方、この時第2コードは第3コードメモリに格納される第3コードとは異なるので、ここでは、正しい翻訳が行われる。分割装置105は、プロセッサ100から生じ制御接続部143により受信される制御信号に応答して、第3コードにより翻訳された全体を、一方で、第2の仕方で暗号化されたメッセージに、他方で第2群識別、すべての使用者識別および使用者公認に分割し、分割装置105は、プロセッサ100の制御の下、第2の仕方で暗号化されたメッセージを第1翻訳装置107に送り、さらに分割装置105は、プロセッサ100の制御の下、第2群識別、すべての使用者識別および使用者公認を接続部126によりデータメモリ106に送る。プロセッサ100は、制御接続部144により、他の（第2群識別が（たとえば、テーブルメモリ108に格納され、制御接続部146により、プロセッサ100に送られる（第1群識別を一致せねばならない）第3群識別と比較することによって）データメモリ106に格納されていることを検出し、その結果、前記データが前記受信装置に意図されていないことが設定される。勿論、前記検出とは別に、第2の仕方で暗号化されたメッセージは一般に、第1翻訳装置107により正しい方法で翻訳され得ない。

【0056】前記受信装置が第1使用者群に属する使用者、この時は非公認に関連するとすれば（送信装置では、メッセージは非公認使用者に関連する暗号化方法により暗号化され、多分さらに他の非公認使用者に関連する暗号化方法により暗号化されるので、前記他の使用者群の残りの公認使用者に関連する暗号化方法により暗号化されない）、図2に示す受信装置の作動は、下記を除いて上記に従う。

【0057】第3テーブルメモリ108は、制御接続部146により、プロセッサ100から生ずる指令信号を受信し、それに応答して、引き続き発生し、接続部128により、第1翻訳装置107に、受信装置を管理す

る非公認使用者に関連する翻訳方法を除いて、非公認使用者に関連する第3コラムに格納される翻訳方法を送る。前記1つの翻訳方法を発生しないのは、たとえば、前記テーブルメモリ108に存在しない前記翻訳方法の結果、または、すべてこれは、明らかに存在するが反対に前記テーブルメモリ108で非活動である前記1つの翻訳方法の結果である。この時、第1翻訳装置107は、前記翻訳方法の1つが得られないので、非公認使用者に関連する翻訳方法による暗号化メッセージの翻訳は果たせない。その結果、もう1つの暗号化メッセージは、暗号化ビデオ信号が翻訳できない翻訳手段102に送られる。

【0058】ペーT Vビデオ信号がアナログ信号であれば、暗号化手段3と翻訳手段102は当業者に周知のフィルムコーダーとフィルムデコーダーである。マルチプレクサー4とデマルチプレクサー101は、たとえば、ビデオ信号とディジタルテレックス信号（また暗号化メッセージと使用者識別等）が組み合わされる、いわゆるテレビジョンチップである。ペーT Vビデオ信号がディジタル信号であれば、暗号化手段3と翻訳手段102は、たとえば、各々、たとえば、たとえば64ビットキーワードの関数として64ビット入力ワードを64ビット出力ワードに変換する、いわゆる、暗号チップと翻訳チップである。暗号化装置6、8、12、15と翻訳装置103、107は、また暗号チップと翻訳チップにより実現される。この場合、従って、メッセージ、暗号化方法および翻訳方法は、いわゆるキーからなる。

【0059】”情報”の概念はできるだけ広い意味を持つように解釈すべきである。したがって、ペーT Vビデオ信号に関するだけでなく、またオプションとして、たとえば、ケーブル網により、航空情報を航空人の家庭に送信することがあり、たとえば、航空人の第1部分は完全に公認され、航空人の第2、第3部分は各々、航空情報の異なる部分についてののみ公認される。これとは別に情報は、たとえば、電気メインにより、使用者の家庭に送信され、この場合、公認使用者のみのボイラーおよび（または）サンスクリーンが駆動されうる。また、”情報へのアクセスを与える、暗号化／翻訳メッセージにより”は、情報源とメッセージ源は地理的に分離されると共に一致するが、ある場合の情報はメッセージに完全に記録されさえされるので（翻訳または非暗号化メッセージは、全部また一部が、情報と一致する）、できるだけ広い意味を持つように解釈すべきである。

【0060】使用者が受信装置を購入または借りる場合には、前記受信装置は一般に、（たとえば、データメモリ106および（または）テーブルメモリ108に格納される）使用者識別と（一般にコードメモリ104に格納される）標準翻訳方法および（または）標準キーを既に備えている。そこで、前記受信装置に送信される第1メッセージは（一般にコードメモリ13および（また

は) 16に格納される) 標準翻訳方法および(または) 標準キーにより、送信装置に暗号化されねばならず、受信装置に翻訳された後、受信装置に、たとえば、(一般に、コードメモリ104に格納される) 新コード、群識別、および、(たとえば、データメモリ106および(または) テーブルメモリ108に格納される) 同じ群に属する使用者の使用者識別、ならびに(たとえば、テーブルメモリ108に格納される) 関連翻訳方法および(または) キー等翻訳メッセージに存在するデータがロードされる。また、受信装置に既に格納されたデータの拡張および(または) 修正および(または) 変型は一般に1つ以上のメッセージにより行われる。この場合、メッセージには表示を備え、この表示は、前記メッセージが主として、翻訳装置107および(または) 翻訳手段102を意図することを表示し、またはメッセージが主としてデータの調節を意図することを表示し、この表示は分割装置105および(または) データメモリ106および(または) プロセッサ100により検出されねばならない。

【図面の簡単な説明】

【図1】 本発明による方法に適用する本発明による送信装置を示す。

【図2】 本発明による方法に適用する本発明による受信装置を示す。

【符号の説明】

1、100…プロセッサ

2…情報源

3…暗号化手段

4…マルチプレクサー

5…メッセージメモリ

6…第1暗号化装置

7…第1テーブルメモリ

8…第2暗号化装置

9…第2テーブルメモリ

10…プロセッサメモリ

11…第1加算装置

12…第3テーブルメモリ

13…第1コードメモリ

14…第2加算装置

15…第4テーブルメモリ

16…第2コードメモリ

20-33、120-125、127、128…接続部

40-54、140-147…制御接続部

101…デマルチプレクサー

102…翻訳手段

103…第2翻訳装置

104…第3コードメモリ

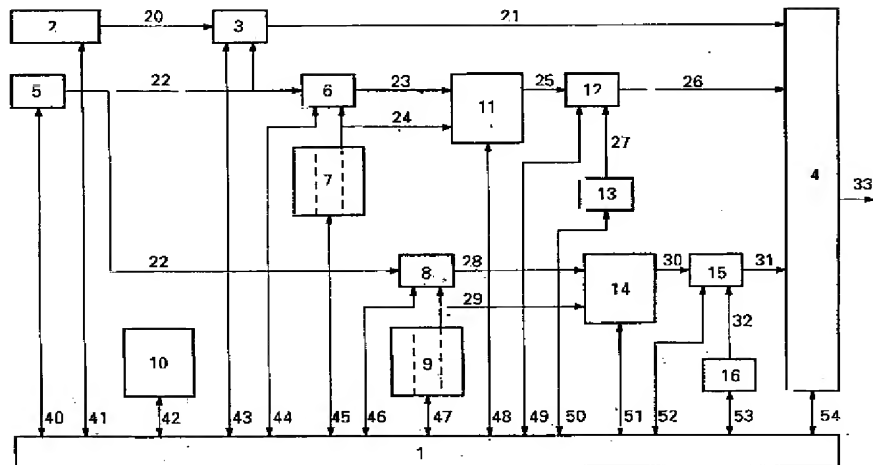
105…分割装置

106…データメモリ

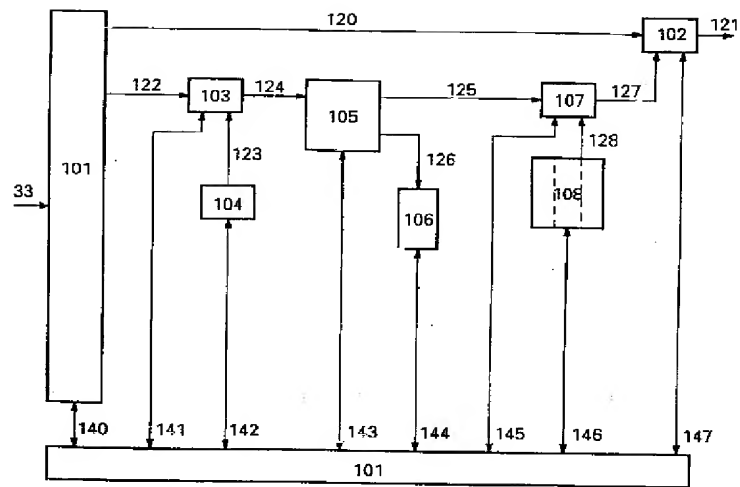
107…第1翻訳装置

108…第3テーブルメモリ

【図1】



【図2】



フロントページの続き

(72)発明者 アンドリース ピーター ヘクストラ  
 オランダ国 2252 ケイエム ボールショ  
 ーテン ルーイス デ コリングニラールン  
 11